UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/689,596	10/22/2003	Donald Yang	BHT-3212-46	6109

7590 09/26/2007

TROXELL LAW OFFICE PLLC
SUITE 1404
5205 LEESBURG PIKE
FALLS CHURCH, VA 22041

EXAMINER	
ABYANEH, ALI S	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/689,596	YANG ET AL.	
	Examiner	Art Unit	
	Ali S. Abyaneh	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 0200*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3, 6-14 and 17-22 are pending.

2. Claims 1, 6, 12-14 and 17-21 are amended.

3. Claims 4, 5, 15, 16 and 23-40 are cancelled.

4. Examiner withdraws objections to claims 13-21 for being of improper dependent form, due to the correction by the applicant.

Response to Arguments

5. Applicant's arguments filed 07-18-2007 have been fully considered but they are not persuasive.

Applicant argues in Kessler "the public key is not chosen from a plurality of universal keys with encoded serial number from the author computer". Examiner respectfully disagrees.

Kesseler discloses client software in a client computer includes a unique secret key (SK) and a unique public key (PK). The client computer further receives a public key (PK) of the receiving computer (column 4, lines 46-54). Kessler teaches obfuscation algorithms O1, O2, DO1 and DO2 are bound within the proprietary client software loaded onto the client computer (column 10, lines 50-52).

Therefore in Kessler the client computer (author computer) includes SK, PK, and PK of the receiving computer, O1, O2, DO1 and DO2 for performing encryption/decryption and obfuscation/de-obfuscation process.

Kessler teaches encrypting digital information using a track key (TK) and encrypting the TK, using the PK of the receiving computer (column 5, lines 30-38).

It is clear from the above citations that the public key (PK) of the receiving computer, which is used to encrypt the TK is within a group of keys in the client computer (author computer), this is functionally equivalent to the applicant's limitation of "choosing one of the plurality of universal keys, and encrypting the content key by the chosen universal key".

Applicant further argues, "..according to Applicant's invention, the encrypting process of the content key also executes the step of storing the encrypted content key and the serial number of the universal key to a header and adding the header in front of the encrypted digital information. However, Kessler discloses that only the encrypted content key is stored in a header portion of a secured file". Examiner respectfully disagrees.

It is well known in the art that a serial number is a series of unique numbers or letters, which are used for identification. It is also well known in the art that in public/private key encryption each public key or private key includes properties and elements, which identifies an entity. In Kessler the public key of the receiver includes properties and elements, which identifies the receiver. In another word the public key of the receiver includes properties or elements that could be considered as a serial number for the public key or the receiver.

Since in Kessler the content key is encrypted by using the public key of the receiver and transmitted to the receiver as a header (column 6, lines 21-29), therefore

the encrypted header inherently includes a serial number of the public key, by broadly interpreting the claim this clearly reads on the limitation of "storing the encrypted content key and the serial number of the universal key to the header".

In view of above discussion examiner maintains the rejection as follows:

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1,11,12 and 22, are rejected under 35 U.S.C. 102(e) as being anticipated by Kessler et al. (US Patent NO. 7,170,999).

Regarding claim 1 and 12

Kessler teaches a digital information protecting method for encrypting a piece of digital information from an author computer (column 2, lines 27-28) with assistances from a server (column 2, lines 31-31), and then transmitting an encrypted digital information to a client computer via a computer network for the client computer to decrypt the encrypted digital information to be used (column 2, lines (column 2, lines 35-40), both the author computer and the client computer

comprising a predetermined information processing software to process the piece of digital information, the information processing software of the author computer comprising a plurality of universal keys with encoded serial number, the method comprising:

in the author computer:

receiving a content key from a server and encrypting the piece of digital information by the content key (column 2, lines 27-33);

choosing one of the plurality of universal keys, and encrypting the content key by the chosen universal key ((column 4, lines 46-54, the public key (PK) of the receiving computer (universal key) is within a group of keys in the author computer),

storing the encrypted content key and the serial number of the universal key to a header, and adding the header in front of the encrypted digital information (column 9, line 54-column 10, line 49); and transmitting the encrypted digital information and the encrypted content key to the client computer (column2, lines 37-40); and in the client computer: decrypting the encrypted content key by a corresponding predetermined key decrypting process; and decrypting the encrypted digital information by the content key to make the piece of digital information can be used by the client computer (column 6, lines 47-65).

Regarding claim 11 and 22

Kessler further discloses a method, wherein the information processing software encrypts and decrypts the piece of digital information by Advanced Encryption Standard; (AES) method (column 6, lines 57-65).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2, 3, 6-10, 13, 14 and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (US Patent NO. 7,170,999), in view of Pensake et al. (US Pub NO. 2001/0052074).

Regarding claim 2 and 13

Kessler teaches all limitation of the claim as applied to claim 1 and 12 above. Kessler does not explicitly teach, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server. However, in an analogous art, Pensak teaches, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server (paragraph [0040]).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kessler to include the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to provide access to encrypted information by authorized user and furthermore to provide a method and system for encrypting electronic information so that access to the information can be controlled by the author or other controlling party (paragraph [0005]).

Regarding claim 3 and 14

Pensake further discloses a method, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized (paragraph [0040]).

Regarding claim 6, 17

Kessler teaches all limitation of the claim as applied to claim 1 and 12 above. Kessler does not explicitly teach, wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission.

However, in an analogous art, Pensak teaches wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission (paragraph [0040]).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kessler to include, before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to provide access to encrypted information by authorized user and furthermore to provide a method and system for encrypting electronic information so that access to the information can be controlled by the author or other controlling party (paragraph [0005]).

Regarding claim 7, 18

Pensake further discloses, wherein the Off-line Access Permission determines whether the client computer is permitted to process and use the received piece of digital information in the off-line situation (paragraph [0040]).

Regarding claim 8-10 and 19-21

Kessler further discloses, wherein the key decrypting process is executed the following steps by the information processing software of the client computer: getting a corresponding universal key according to serial number stored in the header; and decrypting the content key by the universal key; and wherein the information processing software of the client computer downloads the universal key from the server according to the serial number; and wherein the information processing software of the client computer comprises a plurality of universal keys, the information processing software of the client computer chooses corresponding universal key according to the serial number (column 9, line 54-column 10, line 49).

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

AA

Ali Abyaneh
Patent Examiner
Art Unit 2137
09-18-07

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER